James E. Cecchi
CARELLA BYRNE CECCHI
OLSTEIN BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, NJ 07068
(973) 994-1700
Interim Lead Counsel for Plaintiffs
(Additional Counsel on the Signature Page)

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE: AMERICAN MEDICAL COLLECTION AGENCY, INC. CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: All Actions Against CareCentrix (Other Labs Track)	Civil Action No. 19-md-2904 (MCA)(MAH) **SECOND AMENDED CONSOLIDATED CLASS ACTION COMPLAINT: CARECENTRIX**

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(Cont'd)

Page

Plaintiffs, individually and on behalf of classes of all those similarly situated (the "Class" or "Class Members"), upon personal knowledge of the facts pertaining to Plaintiffs and on information and belief as to all other matters, and upon the investigation conducted by Plaintiffs' counsel, bring this class action complaint against CareCentrix, Inc. ("CareCentrix"),[1] and allege as follows:

PRELIMINARY STATEMENT

1. In July 2019, Defendant informed patients to whom it provided various healthcare services that an unauthorized user or users accessed the system run by CareCentrix's billing collections vendor, Retrieval-Masters Creditor's Bureau, Inc., d/b/a American Medical Collection Agency ("AMCA"), between August 2018 and March 2019 (the "Data Breach"). After accessing AMCA's unprotected systems, the hacker exfiltrated the sensitive personal, financial, and medical information of hundreds of thousands of Defendant's patients and sold the information for profit on the illegal marketplace known as the "dark web."

2. Plaintiffs bring this class action because Defendant failed in its basic, legally bound, and expressly-promised obligation to secure and safeguard its patients' protected health information ("PHI") and personally identifiable information ("PII")—such as Plaintiffs' and Class Members' names, mailing addresses, phone numbers, dates of birth, Social Security numbers, information related to Plaintiffs' and Class Members' medical providers and services (such as dates of service, tests ordered, diagnosis codes that represent conditions and diseases, and referring doctor) and other private information—such as credit and debit card numbers, bank account

[1] As additional facts come to light, Plaintiffs may respectfully seek leave to amend this Complaint in order to bring additional causes of action by plaintiffs from other states.

information, insurance, insurance subscriber identification number (all collectively referred to as "Personal Information").

3. As of today, approximately 500,000 CareCentrix patients have had their Personal Information compromised as a result of the Data Breach. As a result of Defendant's failure to protect the consumer information it was entrusted—and legally obligated—to safeguard, Plaintiffs and Class Members suffered a loss of value of their Personal Information and have been exposed to and are at imminent and significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. In fact, numerous Class Members are already victims of fraud.

4. Defendant has a duty to safeguard and protect customer information entrusted to it and could have prevented this theft had it limited the Personal Information of its patients that it shared with its vendors and business associates and employed reasonable measures to assure its vendors and business associates implemented and maintained adequate data security measures and protocols to secure and protect customers' Personal Information.

5. Plaintiffs and Class Members entrusted Defendant with, and allowed Defendant to gather, highly sensitive information relating to their health and other matters as part of seeking healthcare benefits. They did so in confidence, and they had the legitimate expectation that Defendant will respect their privacy and act appropriately, including only sharing their information with vendors and business associates who legitimately needed the information and were equipped to protect it.

6. Trust and confidence are key components of Plaintiffs' and Class Members' relationship with Defendant. Without it, Plaintiffs and Class Members would not have provided Defendant with, or allowed Defendant to collect, their most sensitive information in the first place.

To be sure, Plaintiffs and Class Members relied upon Defendant to keep their information secure, as they are required by law to do.

7. Defendant's intentional, willful, reckless, and/or negligent conduct—failing to prevent the Data Breach, failing to limit its severity, failing to detect it in a timely fashion, and failing to timely notify Plaintiffs and the Class—damaged Plaintiffs uniformly. As discussed herein, fraudulent activities have already been linked to Defendant's conduct. For this reason, Defendant should pay for appropriate identity-theft protection services and reimburse Plaintiffs and the Class for the costs caused by Defendant's sub-standard security practices and failure to timely disclose the same. Plaintiffs and the Class are, therefore, also entitled to injunctive and other equitable relief that safeguards their information, requires Defendant to significantly improve its security, and provides independent, expert oversight of Defendant's security practices with respect to its vendors and business associates.

8. Defendant has also been unfairly and unjustly enriched as a result of its improper conduct, such that it would be inequitable for it to retain the benefits conferred upon it by Plaintiffs and the Class Members. Plaintiffs never would have engaged CareCentrix to perform medical services and entrusted Defendant with their Personal Information, had they known that Defendant would permit unauthorized access to their Personal Information by Defendant's complete and utter disregard for security safeguards and protocols. Plaintiffs would have used another provider.

JURISDICTION AND VENUE

9. This Second Amended Consolidated Complaint is intended to serve as an administrative summary as to all other complaints consolidated in this multidistrict litigation asserting claims against CareCentrix and shall serve for all purposes as an administrative device

to aid efficiency and economy for the Class defined below. As set forth herein, this Court has general jurisdiction over Defendant and original jurisdiction over Plaintiffs' claims.

10. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, there are more than 100 putative Class Members, and minimal diversity exists as Defendant and at least one Class Member are citizens of different states.

11. This Court has personal jurisdiction over Defendant because it maintains sufficient minimum contacts in New Jersey such that it intentionally avails itself of this Court's jurisdiction by conducting operations here and contracts with companies in this District. Additionally, the United States Panel on Multidistrict Litigation transferred all related matters to this District, so Plaintiffs are bringing their claims against Defendant in this litigation before this Court.

12. Venue is proper in this District pursuant to 28 U.S.C. § 1407 and the July 31, 2019 Transfer Order of the Judicial Panel on Multidistrict Litigation in MDL 2904 or, in the alternative, pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the conduct alleged herein occurred in, were directed to, and/or emanated from this District. Venue is additionally proper because Defendant transacts business and may be found in this District.

NAMED PLAINTIFFS

13. Plaintiffs are individuals who, upon information and belief, had their Personal Information compromised in the Data Breach, and bring this action on behalf of themselves and all those similarly situated both across the United States and within their State or Territory of residence. These allegations are made upon information and belief derived from, *inter alia*, counsel's investigation, public sources—including sworn statements, Defendant's website, and the facts and circumstances currently known. Because Defendant has exclusive but incomplete

knowledge of what information was compromised for each individual, including PHI, Plaintiffs reserve the right to supplement their allegations with additional facts and injuries as they are discovered.

14. Plaintiff Brian D. Graifman ("Graifman") is a citizen and resident of the state of New York.

15. CareCentrix provided Plaintiff Graifman with coordinated healthcare benefits, including medical monitoring services, in connection with his use of a continuous positive airway pressure ("CPAP") device that Graifman received from Landauer Medstar ("Landauer").

16. Either Landauer contracted with CareCentrix to perform the monitoring services and, on information and belief, provided CareCentrix with Graifman's Personal Information or Plaintiff Graifman indirectly provided CareCentrix with his Personal Information since Landauer contracted with CareCentrix to provide Graifman with CPAP monitoring services.

17. On information and belief, Plaintiff Graifman's bill from CareCentrix was subsequently sent to Defendant's billing-collections vendor, AMCA.

18. As part of billing-collections services provided for Defendant, Plaintiff Graifman has been contacted by AMCA through several letters, including on or around February 13, 2017, 2017, March 13, 2017, and April 13, 2017.

19. On July 10, 2019, Plaintiff Graifman received a notice from CareCentrix informing him of the Data Breach at AMCA, which included the compromise of his Personal Information provided to AMCA by CareCentrix.

20. As a CareCentrix patient, Plaintiff Graifman believed that CareCentrix would protect his Personal Information, once it was provided to CareCentrix or its vendors.

21. Plaintiff Graifman would have ensured that his Personal Information was not provided to CareCentrix had he known that it would fail to protect his Personal Information.

22. Plaintiff Graifman suffered and will continue to suffer damages due to the Data Breach. Following the Data Breach, Plaintiff Graifman began receiving suspicious phishing telephone calls and text messages. Plaintiff Graifman's Personal Information was also discovered for sale on a dark web marketplace along with other victims of the Data Breach.

23. In June 2021, as a result of the Data Breach, Graifman was the victim of at least one fraudulent charge for a product called Vitamix in the amount of approximately $653.20 (that he did not pay) on his credit card, which was the same credit card used for expenses from Landauer and/or CareCentrix and provided to AMCA. As a result, he was forced to close his credit card account and open a new one.

24. Plaintiff Graifman has spent substantial time mitigating the adverse consequences of the Data Breach. To date, Plaintiff Graifman has spent several hours going over his old credit card statements during the relevant breach period. In addition, Plaintiff Graifman has had to maintain his credit card monitoring service that he was planning on cancelling prior to the Data Breach. Plaintiff Graifman will have to spend considerable time going forward monitoring for potential adverse consequences from the Data Breach, including, without limitation, credit card theft, identify theft, false-tax-return information submitted, false loans submitted, expenses for credit monitoring, expenses for lifting credit-security freezes, and reduced credit scores.

25. Plaintiff Debbie Amico ("Amico") is a citizen and resident of the state of Florida.

26. Plaintiff Amico received coordinated healthcare benefits from CareCentrix.

27. Plaintiff Amico provided CareCentrix with her Personal Information as part of receiving coordinated healthcare benefits.

28. On information and belief, Plaintiff Amico's bill from CareCentrix was subsequently sent to Defendant's billing-collections vendor, AMCA.

29. On July 10, 2019, Plaintiff Amico received a notice of the Data Breach at AMCA in connection with CareCentrix, stating that Plaintiff Amico's Personal Information may have been compromised.

30. As a CareCentrix patient, Plaintiff Amico believed that CareCentrix would protect her Personal Information, such as diagnostic information, once she provided it to CareCentrix or its vendors.

31. Plaintiff Amico would not have provided CareCentrix with her Personal Information or used CareCentrix to provide coordinated healthcare benefits had she known that it would fail to protect her Personal Information.

32. Plaintiff Amico suffered and will continue to suffer damages due to the Data Breach. In late 2019, Plaintiff Amico was the victim of at least one fraudulent charge at Sam's Club (that she did not pay) on her credit card, which was the same credit card used for expenses from CareCentrix and provided to AMCA

33. Plaintiff Amico has spent substantial time mitigating the adverse consequences of the Data Breach. To date, Plaintiff Amico has spent several hours trying to speak with AMCA or its representatives about the Data Breach, and she has spent at least one hour per week monitoring her credit and financial accounts for any unauthorized activity. Plaintiff Amico will have to spend considerable time going forward on monitoring for potential adverse consequences from the Data Breach, including, without limitation, credit card theft, identify theft, false-tax-return information submitted, false loans submitted, expenses for credit monitoring, expenses for lifting credit-security freezes, and reduced credit scores.

34. Plaintiff L.D., a minor by and through her mother and guardian Andrea Dominguez ("Dominguez"), is a citizen and resident of the state of Florida. Plaintiff L.D. makes all the following allegations in this complaint by and through her mother and guardian, Dominguez, who is also a citizen and resident of the state of Florida.

35. Plaintiff L.D. received coordinated healthcare benefits from CareCentrix through her healthcare provider beginning on or about June 1, 2017.

36. Plaintiff L.D. provided CareCentrix with her Personal Information as part of obtaining coordinated health care benefits.

37. The bill to Plaintiff L.D. from CareCentrix was subsequently sent to Defendant's billing-collections vendor, AMCA.

38. As part of billing-collections services provided for Defendant, Plaintiff L.D. has been contacted by AMCA through several letters, including on or around July 16, 2018, and August 27, 2018, and in response, Plaintiff L.D. (by and through her mother and guardian Dominguez) provided Personal Information to AMCA.

39. On July 10, 2019, Dominguez received a letter for Plaintiff L.D. regarding a notice of data breach involving AMCA in connection with CareCentrix, stating that Plaintiff L.D.'s Personal Information may have been compromised.

40. As a CareCentrix patient, Plaintiff L.D. believed that CareCentrix would protect her Personal Information once she provided it to CareCentrix or its vendors.

41. Plaintiff L.D. would not have provided CareCentrix with this Personal Information or used CareCentrix to provide coordinated healthcare benefits had she known that it would fail to protect her Personal Information.

42. Plaintiff L.D. suffered and will continue to suffer damages due to the Data Breach. Following the Data Breach, Plaintiff L.D.'s Personal Information was discovered for sale on a dark web marketplace along with other victims of the Data Breach. As a child, Plaintiff L.D.'s Personal Information is particularly attractive to identity thieves because her credit history represents a clean slate that will remain untouched until she reaches the age of majority. As a result, Plaintiff L.D. is at a particularly high risk of future identity theft and fraud, which, due to her young age, may affect her ability to build and obtain credit for the rest of her life.

43. Plaintiff L.D. will have to spend considerable time going forward on monitoring for potential adverse consequences from the Data Breach, including, without limitation, credit card theft, identify theft, false-tax-return information submitted, false loans submitted, expenses for credit monitoring, expenses for lifting credit-security freezes, and reduced credit scores.

44. Plaintiff Dominguez, who also brings claims against Defendant on her own behalf, is a citizen and resident of the state of Florida.

45. Plaintiff Dominguez purchased coordinated healthcare benefits from CareCentrix on behalf of her minor daughter, Plaintiff L.D., through Plaintiff L.D.'s healthcare provider.

46. Plaintiff Dominguez's credit card information was provided to CareCentrix as part of obtaining coordinated healthcare benefits on behalf of her minor daughter, Plaintiff L.D.

47. The bill to Plaintiff L.D. (paid by Plaintiff Dominguez) from CareCentrix was subsequently sent to Defendant's billing-collections vendor, AMCA.

48. As part of billing-collections services provided for Defendant, Plaintiff L.D. has been contacted by AMCA through several letters, including on or around July 16, 2018 and August 27, 2018 and, in response, Plaintiff Dominguez provided her credit card information to AMCA.

49. On July 10, 2019, Plaintiff Dominguez received a letter for Plaintiff L.D. regarding a notice of data breach involving AMCA in connection with CareCentrix, stating that Plaintiff Dominguez's financial information may have been compromised.

50. In providing her financial information to CareCentrix, Plaintiff Dominguez believed that CareCentrix would protect her financial information once she provided it to CareCentrix or its vendors.

51. Plaintiff Dominguez would not have provided CareCentrix with her financial information or used CareCentrix to provide coordinated healthcare benefits to her daughter had she known that it would fail to protect her financial information.

52. During 2018 and 2019, Plaintiff Dominguez received suspicious phishing calls from a company fraudulently claiming to collect money for AMCA and asking for her credit card number. In September 2019, as a result of the Data Breach, Plaintiff Dominguez experienced at least one fraudulent charge for fast food of approximately $48 (that she did not pay) on her credit card, which was the same card used for expenses for Plaintiff L.D. (among other expenses), including being provided to AMCA for CareCentrix bills. As a result of the Data Breach, Plaintiff Dominguez has changed her credit card information in response to fraudulent activity.

53. Plaintiff Dominguez has spent substantial time mitigating the adverse consequences of the Data Breach. To date, she has spent several hours trying to speak with AMCA and CareCentrix representatives about the Data Breach and at least one hour per week monitoring credit and financial accounts for any unauthorized activity.

DEFENDANT CARECENTRIX

54. Defendant CareCentrix is incorporated in the State of Delaware and is a health services management company with its headquarters at 20 Church Street in Hartford, Connecticut.

FACTUAL ALLEGATIONS

A. The Data Breach Impacted Patients of a Wide Variety of Healthcare Organizations, Including CareCentrix

55. From at least August 1, 2018 to March 30, 2019, an unauthorized user or users gained access to the AMCA system that contained information obtained from various entities, including CareCentrix, as well as information that AMCA collected itself. This date range is limited by the scope of AMCA's investigation and AMCA's lack of historical logging and monitoring of activity on its systems.

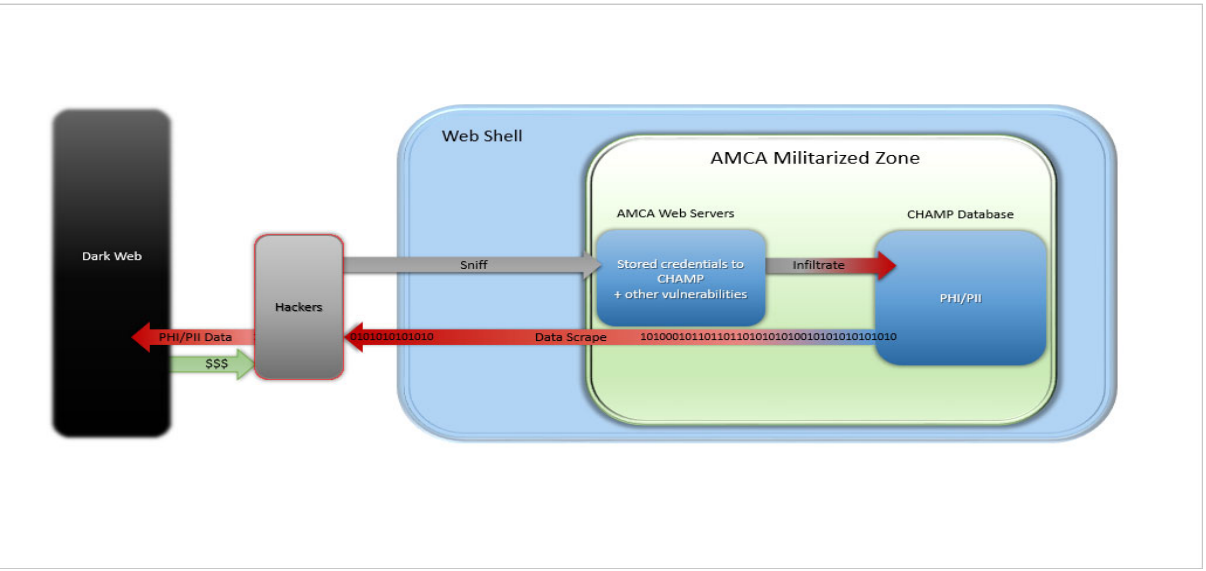
56. Approximately 500,000 CareCentrix patients have been affected by the Data Breach, making it one of the largest health-related data breaches reported to the U.S. Department of Health and Human Services ("HHS") in 2019.[2] The overall AMCA Data Breach (including all impacted laboratories) was the second largest to be reported since HHS's Office for Civil Rights launched its breach portal in 2010.[3]

57. Upon information and belief, and based upon the limited documents produced to date, the hackers were able to exploit easily-recognizable vulnerabilities in the AMCA IT infrastructure to perpetrate the Data Breach. Below is a high-level sketch of how the Data Breach occurred:

---

[2] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,* U.S. Dep't of Health and Human Services, Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Oct. 9, 2019); *see also August 2019 Healthcare Data Breach Report*, HIPAA Journal, https://www.hipaajournal.com/august-2019-healthcare-data-breach-report/ (last visited Oct. 9, 2019).

[3] *July-reported healthcare breaches exposed 22 million people's data*, Modern Healthcare, https://www.modernhealthcare.com/cybersecurity/july-reported-healthcare-breaches-exposed-22-million-peoples-data (last visited Oct. 9, 2019).



58. Prior to the discovery of the Data Breach, Nuvei (a payment processor) alerted AMCA of a potential compromise of credit cards processed by AMCA. This alert prompted AMCA to hire End Point Corporation ("End Point"), a software development and hosting provider, to perform an audit. End Point's audit found the presence of malicious scripts, outdated software, security and privacy settings that were below industry standard, and a lack of compliance with the PCI-DSS standards and HIPAA.

59. After the Data Breach was discovered, Charles River Associates, a consulting firm engaged by AMCA, provided a "forensic analysis" of the AMCA system. Charles River conducted a limited investigation and nevertheless concluded that [redacted][4]

60. Specifically, the evidence shows that [redacted][5] Web shells are pieces of code placed on a web

[4] [redacted] (emphasis added).

[5] *Id.*

application server to provide an interface for a remote attacker to execute commands. An attacker attaches an executable script, here in the PHP coding language, to the web server and the script searches for vulnerabilities in a web server's systems. The web shell can also execute commands and upload and download files. Web shells are only possible if the web application or server contain vulnerabilities such as insecure or poorly written code, a misconfiguration, credentials that are unencrypted, a lack of security patching, or minimal segmentation between different areas in a network. Moreover, web shells leave contemporaneous evidence of their activities, referred to as "noise," but AMCA did not capture this because it was not logging the traffic on its web servers and it did not employ a Web Application Firewall. Additionally, commercial scanning tools and anti-virus software can detect and prevent the installation of web shells, but AMCA did not employ them here.

61. By installing the web shell, threat actors were able to get inside AMCA's consumer database and possibly the entire organization's network. From there, they were able to exploit the unpatched and out-of-date AMCA IT systems to perpetrate the Data Breach.

62. Specifically, threat actors found the following [redacted]:[6]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

c. [redacted]

[redacted];

[redacted]

and

[redacted]

63. These security vulnerabilities existed because AMCA's web servers used systems that were out of date, unpatched, untested, and were not "hardened," i.e., fortified using appropriate security measures. AMCA ran an unsupported and vulnerable version of PHP, an open-source coding language. As an End Point security review acknowledged in a March 2019 report to AMCA, there was a need to "upgrade to latest PHP." In March 2020, amcaonline.com still showed an unpatched version of Apache and an unpatched version of MySQL.

64. Further, AMCA failed to patch and upgrade its IT systems. This is a basic feature of IT security. It is well known in the industry that threat actors learn of vulnerabilities in IT systems and exploit them if they are not patched, and even basic IT security requires constant patching and updating as potential vulnerabilities become known. Further, because AMCA's web server was publicly available on the Internet, attackers could scan it and learn that it utilized unpatched and out-of-date software.

65. As a result, AMCA's system was not a difficult system to attack; threat actors could have discovered the vulnerabilities through simple open-source tools from the Internet and commercially available hacking tools.

66. Once threat actors were inside AMCA's systems, they were not detected, in part, because:

a. AMCA was not running an antivirus scanner or a scan of its file system to

detect known malware; and

b. AMCA's Security Information and Event Management (SIEM) was ineffective because it was not logging activities on its servers.

67. Even if an attacker was able to gain access to AMCA's systems via a web shell, an effective IT system needs to provide additional security so as to protect the most important (and desirable) information. Additional security measures include taking steps to segregate the most sensitive systems from less sensitive systems and limiting access to all systems, especially sensitive systems. For AMCA, the CHAMP database stored patient PII/PHI and was the most important system to protect. Information contained in the CHAMP database included:

- Patient names
- Patient addresses
- Patient contact phone numbers (up to three)
- Patient Social Security numbers
- Patient dates of birth
- Guarantor/responsible party names
- Guarantor/responsible party name addresses
- Guarantor contact phone numbers (up to three)
- Guarantor / responsible party Social Security numbers
- Subscriber member
- Referring physician name
- Insurance designation flag
- Insurance group number and insurance ID
- Medicare / Medicaid number
- Patient/subscriber account number
- Specimen collection date
- Dates of service
- Specimen number
- Patient ID
- Invoice/requisition numbers
- Clinical information
- ICD and diagnosis codes
- Test order names
- Test order results
- Photographs taken for paternity identity testing

68. However, instead of providing additional layers of security to the CHAMP database, AMCA made the CHAMP database readily accessible from the Internet. Additionally, the CHAMP database was supposed to be segregated from the rest of AMCA's IT system, but it was not.

69. In practice, what this meant was that, once hackers were inside AMCA's systems, they could easily traverse from the web server to the CHAMP database. This lateral movement was made even easier by the fact that AMCA left stored credentials (i.e., user name and passwords) accessible ***and*** threat actors were able to override system requirement to enter authorizations required to access the CHAMP database. The Charles River timeline reveals that once threat actors entered the AMCA system as early as August 1, 2018, without detection, they were able to "sniff and scrape"—i.e. monitor what was going on in the system ("sniff") and exfiltrate information ("scrape"). [redacted].[7]

70. [redacted].[8] Specifically, threat actors downloaded files containing collection letters, access lists, credentials, a list of transactions, among other things.

71. On January 27, 2019, threat actors inserted another web shell without detection.

72. On March 11, 2019 and March 29, 2019, threat actors downloaded several files from AMCA without detection. Specifically, threat actors were able to exfiltrate 14 files on March 11, 2019, including access lists and user credentials. And on March 29, 2019, threat actors exfiltrated another 40 files.

---

[7] [redacted].

[8] [redacted]

73. At no point did AMCA discover the threat actors—not upon entry, not when they traversed the system, not when they overrode the requirement for a user to authenticate themselves, and not when they exfiltrated files.

B. AMCA's 2019 Audit Revealed Serious Vulnerabilities That It Did Not Remediate

74. End Point's March 2019 audit of AMCA revealed numerous un-remediated deficiencies. First, AMCA was using a Linux operating system that had not been updated or patched and was relying on a 2015 version of the software.

75. Further, the production database server was devoid of network segmentation between the web server that was publicly exposed and the underlying database. AMCA also failed to follow recommended security practices on its MySQL program. In layman's terms, this meant that compromising the public-facing web server allowed threat actors to compromise the underlying, non-publicly facing, database server containing the PII and PHI at issue in this case.

76. End Point had to upgrade AMCA's firewall policies and found malicious scripts on AMCA's webserver. End Point could not tell how long malicious, undetected scripts had been present because AMCA failed to have the requisite Web Application Firewall installed and was not logging traffic on the web server. End Point needed to remediate both of these deficiencies, as well as install an antivirus scanner and new rules and controls to prevent SQL injections.

77. During this period, available network logs showed that a "keylogger"—a program that tracks what keys are pressed—had been installed on a Mac device in AMCA's finance/accounting department since March 7, 2018, seven months before evidence of a web shell was found on the web server. The keylogger made multiple successful connections to an external IP address. The user who operated the compromised Mac device worked in AMCA's finance department and thus had ready access to AMCA's accounting system that processed credit card

payments. The End Point auditor wrote: "we should make the assumption that someone could've obtained any passwords typed into this machine and potentially any data on it." And "the fact that they were able to run code, means they could've ran anything they wanted, so yes, they could've obtained full access to that Mac, and moved laterally through the network to anything else connected."

C. Threat Actors Sold Class Members' Personal Information on the Dark Web

78. Following the Data Breach, there was evidence that the exfiltrated PII and PHI was available on the dark web and in fact being used to commit fraud.

79. Specifically in November 2018, after forensic evidence proved that files were exfiltrated by threat actors, GlobalOnePay contacted AMCA and informed AMCA that [redacted][9] This was done via a "common point of purchase," which is a way for credit card issuer banks to trace fraud associated with the use of their cards.

80. At that time, Conformance Tech noted that there were a "small number of cards [that had fraud on them], BUT, it is from a really small card issuer. Small banks and Discover [credit cards] tend to be leading indicators of larger problems."[10]

81. In response, AMCA conducted an internal review and concluded that no one had accessed credit card data from its systems because there was "evidence of this shown in our exhaustive review."[11]

---

[9] [redacted]

[10] AMCAPROD138907.

[11] *Id.*

82. On February 13, 2019, GlobalOnePay contacted AMCA again about another common point of payment ("CPP") alert involving fraud on 22 credit cards.[12] AMCA again took the position that there had not been a data breach.

83. On February 25, 2019, Nuvei, a payment technology partner, informed AMCA that New York Community Bank notified Nuvei that 88 credit cards were compromised between December 26, 2017 and December 17, 2018.[13]

84. At the end of February 2019, Gemini Advisory, a New York-based company that works with financial institutions to monitor the sale of consumer information on underground markets, ***identified a large number of compromised AMCA patient information for sale on the dark web***.[14] As reported on May 10, 2019, by DataBreaches.net:

> On February 28, 2019, Gemini Advisory identified a large number of compromised payment cards while monitoring dark web marketplaces. Almost 15% of these records included additional personally identifiable information (PII), such as dates of birth (DOBs), Social Security numbers (SSNs), and physical addresses. A thorough analysis indicated that the information was likely stolen from the online portal of the American Medical Collection Agency (AMCA), one of the largest recovery agencies for patient collections. Several financial institutions also collaboratively confirmed the connection between the compromised payment card data and the breach at AMCA.[15]

---

[12] AMCAPROD0215349.

[13] AMCAPROD1117103.

[14] Gemini Advisory, *AMCA Breach May be Largest Medical Breach in 2019* (June 4, 2019), available at https://geminiadvisory.io/amca-largest-medical-breach/ (last visited Mar. 21, 2022).

[15] Databreaches.net, *American Medical Collection Agency breach impacted 200,000 patients – Gemini Advisory* (posted May 10, 2019), available at https://www.databreaches.net/american-medical-collection-agency-breach-impacted-200000-patients-gemini-advisory/ (last visited Mar. 21, 2022).

85. Gemini's additional research revealed AMCA's exposure window had lasted for at least seven months beginning in September 2018.[16]

86. The combination of AMCA-related PII being for sale on the dark web and the notifications that AMCA received definitively shows that the threat actors, after exfiltrating PII and PHI from AMCA's systems, sold the information on the dark web and purchasers of that information subsequently committed credit card fraud.

87. On March 1, 2019, Gemini Advisory attempted to notify AMCA, but as Gemini Advisory reportedly told DataBreaches.net, "they did not get any response to phone messages they left." Failing to obtain any response from AMCA, Gemini Advisory "promptly contacted federal law enforcement, which reportedly followed up by contacting AMCA."[17]

88. Following notification from law enforcement, AMCA's payment portal became unavailable for weeks.[18]

89. In its notice to patients affected by the Data Breach, AMCA claims it learned of the unauthorized access on March 20, 2019. Yet, CareCentrix failed to take any steps to notify patients whose Personal Information was affected until months later.

90. In a written statement attributed to AMCA in June 2019, AMCA announced it was still investigating the Data Breach:

> We are investigating a data incident involving an unauthorized user accessing the American Medical Collection Agency system," reads a written statement attributed to the AMCA. "Upon receiving information from a security compliance firm that works with credit card companies of a possible security compromise, we conducted an internal review, and then took down our web payments page.
> . . . .

16 *Id.*

17 *Id.*

18 *Id.*

> We hired a third-party external forensics firm to investigate any potential security breach in our systems, migrated our web payments portal services to a third-party vendor, and retained additional experts to advise on, and implement, steps to increase our systems' security. We have also advised law enforcement of this incident. We remain committed to our system's security, data privacy, and the protection of personal information.[19]

91. On June 17, 2019, AMCA filed for Chapter 11 bankruptcy in the Southern District of New York stating its intention to liquidate. The bankruptcy filings describe the types of Personal Information maintained by AMCA, as well as additional specifics regarding the Data Breach. According to an affidavit submitted by Russell H. Fuchs, the Chief Executive Officer of AMCA:

> [AMCA] by its very nature, requires it to collect and maintain data transmitted to it by its clients that includes personally identifiable information about third-party debtors that could include names, home addresses, Social Security numbers, bank account information for consumers choosing to pay online by check and, for consumers choosing to pay their outstanding balances by credit card, credit card information. In the case of the AMCA business, that information might also include dates of birth and certain medical information related to any laboratory tests for which payment is sought. In all, at any given time, [AMCA] would have held tens of millions of individual points of data regarding millions of individual persons, none of which could be handled without a robust IT system.
>
> [AMCA]'s original IT architecture was built around an IBM mainframe-based system that ran on COBOL4 and served the [AMCA]'s purposes well for many years. However, with ever-increasing market demands for enhanced interconnectivity between the [AMCA]'s and its clients' systems, as well as for web-based interaction with both the [AMCA]'s clients and its clients' consumer and patient-debtors, it was clear that continued reliance on the [AMCA]'s internet-unconnected mainframe system would not be tenable in the long term.
>
> Accordingly, in 2015, after several years of internal planning and development, the [AMCA] began to transition to a proprietary, server-

[19] *LabCorp: 7.7 Million Consumers Hit in Collections Firm Breach, Krebs on Security* (June 4, 2019), https://krebsonsecurity.com/2019/06/labcorp-7-7m-consumers-hit-in-collections-firm-breach/; *see also Information about the AMCA Data Security Incident*, LabCorp, https://www.labcorp.com/AMCA-data-security-incident (last updated June 10, 2019).

> based, network-connected system. [AMCA] invested over a million dollars in the new system, employing outside IT consultants to ensure that the system would reflect current technological standards, including, importantly, appropriate data security protocols.[20]

92. Despite touting its investment in data security, AMCA subsequently acknowledged that it "first learned that there might be a problem" when it received a series of notifications that "suggested that a disproportionate number of credit cards that at some point had interacted with the [AMCA's] web portal were later associated with fraudulent charges."[21]

93. In response, AMCA "shut down its web portal to prevent any further compromises of customer data, and engaged outside consultants who were able to confirm that, in fact, [AMCA]'s servers … had been hacked as early as August, 2018." AMCA explained that "the breach required [AMCA] to hire IT professionals and consultants from three different firms, to identify the source of the breach, diagnose its cause, and implement appropriate solutions. To date, these expenses alone cost approximately $400,000, and have effectively shut down outside entry into [AMCA]'s IT network by severely restricting access via the employment of individual authentication mechanisms, VPN access, or specifically vetted 'whitelists' of pre-approved IP's."[22]

94. AMCA stated that the costs of providing notice to affected individuals, coupled with the loss of its largest clients, required it to reduce its workforce from 113 employees at year-end 2018 to just 25 employees as of June 17, 2019. As a result, AMCA stated it "no longer is optimistic that it will be able to rehabilitate its business."

---

20 *In re Retrieval-Masters Creditors Bureau, Inc*., No. 7:19-bk-23185, Dkt. Entry 2 (Bankr. S.D.N.Y. June 17, 2019).

21 *Id*.

22 *Id*.

95. While AMCA was able to absolve itself of liability by declaring bankruptcy, there are strong indications that the information exfiltrated from AMCA's database is still being offered for sale on underground markets. A compiled list containing information of more than 60 individuals from varying geographic regions and demographics who had their information stored on AMCA's database was searched across dark web markets notorious for selling confidential Personal Information acquired from threat actors and malicious hackers. Of this sample, more than 87% had their information offered for sale by *two single vendors* on just *one* popular dark web market. It is highly unlikely that information associated with such a significant percentage of the sample would be available through two vendors unless the data was obtained from the same breach—a significant indication that *all* Plaintiffs and Class Members had their Personal Information accessed, exfiltrated, and then disseminated by unauthorized parties. Given the vastness of the dark web, there is high probability that each Plaintiff's and Class Member's data is available for sale.

D. CareCentrix's Patients' Information Was Exposed by the Data Breach

1. CareCentrix Obtained Personal Information of Plaintiffs and Class Members and Shared That Information With AMCA

96. CareCentrix provides health benefits management services to more than 26 million people by connecting providers and patients through a national network of more than 8,000 credentialed providers throughout the country.[23] It claims to be uniquely "set apart" to provide post-acute care and "support and coordination for patients and their families throughout care transitions, including, among other things, "Home Sleep Services." [24] CareCentrix offers post-

[23] https://finance.yahoo.com/news/lawsuit-hundreds-employees-health-management-051353574.html (last accessed Aug. 7, 2019).

[24] https://www.carecentrix.com/about-us (last accessed Aug. 7, 2019).

acute care to patients by providing programs to "improve quality and lower costs by allowing patients to heal or age where they want to be: at home."

97. Upon information and belief, CareCentrix charges patients for the services it provides to them and its invoices include only fees for such services. Patients are responsible for paying CareCentrix for performing services either through their insurance or out-of-pocket, if the patient does not have insurance or the costs are not entirely covered by insurance.

98. If CareCentrix's patients fail to pay their invoices within a specified time, CareCentrix employs an associated business for collection. Beginning in at least 2014 and throughout the relevant time period, CareCentrix utilized AMCA as a billing collection agency.

99. Upon information and belief, in order to facilitate collection, CareCentrix regularly provided AMCA with its patients' Personal Information, which AMCA in turn stored in its own computer systems. In addition, as part of AMCA's billing collection services for CareCentrix, Plaintiffs furnished Personal Information directly to AMCA, which AMCA subsequently stored.

2. CareCentrix Informs Patients That They Were Impacted by the Data Breach

100. CareCentrix began informing its patients in or around July 2019 that AMCA had been subject to a "data privacy incident" and that the Data Breach may have included their PII and PHI including name, identity of medical providers, and dates of service.

101. CareCentrix also informed its patients that the AMCA Data Breach, which compromised their PII and PHI, occurred between August 1, 2018 and March 30, 2019.

102. On July 11, 2019, CareCentrix advised the Office of Civil Rights ("OCR") of the Data Breach and reported that 467,621 individuals were impacted, this, despite the fact that CareCentrix knew, or should have known, of the Data Breach on March 20, 2019.

103. CareCentrix failed to provide proper, timely notice of the Data Breach sufficient to allow its patients to take steps to protect themselves and their Personal Information.

104. Despite the fact AMCA was notified of the Data Breach on March 20, 2019, CareCentrix knew or should have known of the Data Breach at or near that time, yet did not notify its patients until July 2019.

3. CareCentrix Committed to Safeguarding its Patients' Personal Information

105. CareCentrix agreed that it was bound to the privacy and security policies of the health care plans concerning its patients and that its Privacy Policy supplemented each health care plan policy pursuant to CareCentrix's Customer Agreements with those health care plans.

106. CareCentrix's Privacy Policy—available via its website—applies to all information collected by its website, mobile applications, and online services that operate and link to the Privacy Policy (such as a patient portal, allowing individuals to pay their bills online). CareCentrix's Privacy Policy, like any privacy policy, acknowledges that no website is 100% secure, but that it would at least "take reasonable precautions to safeguard the Personal Information transmitted between visitors and the Services and the Personal Information stored on our servers."[25] In instances where CareCentrix could not guarantee that transmittals of data would be "100% secure," it encouraged users to use its website to communicate, rather than email correspondence, since its website was more secure.[26]

---

[25] CareCentrix Privacy Policy, https://www.carecentrix.com/privacy-policy (last accessed Nov. 9, 2019).

[26] *Id.*

107. CareCentrix thus provided patients, including Plaintiffs and Class members, with a false sense of security that, by using its website, patients would have a more secure way of providing their Personal Information to CareCentrix.

108. In a September 27, 2018 press release, CareCentrix touted its data security:

> CareCentrix, a leading provider of post-acute care management, announced that several of their technology platforms used to store, process, maintain, and transmit customer electronic protected health information (ePHI)* have earned Certified status for information security by HITRUST. HITRUST CSF Certified status demonstrates that the CareCentrix technology platforms*, which are used to store, process, maintain, and transmit customer ePHI, have met key regulatory requirements, industry defined requirements, and are appropriately managing risk.[27]

109. CareCentrix further claimed that meeting the above standards placed it in an "elite" group of organizations that have earned this certification which, according to John Driscoll, CareCentrix's Chief Executive Officer, represented the "gold-standard" of security.[28] This certification furthermore demonstrates CareCentrix's commitment to "patient data privacy and safety."[29]

110. These statements were untrue and in stark contrast to the negligent way CareCentrix treated Class Members' Personal Information in providing it to AMCA.

111. In addition, HIPAA requires that CareCentrix provide every patient it treats, including Plaintiffs and the putative Class Members, with a privacy notice. In CareCentrix's Notice of Privacy Practices, CareCentrix states that it uses PII and PHI for limited purposes,

---

[27] Press Release, CareCentrix Achieves HITTRUST CSF Certification to Manage Risk, Improve Security Posture and Meet Compliance Requirements (Sept. 27, 2018), *available at* https://markets.businessinsider.com/news/stocks/carecentrix-achieves-hitrust-csf-certification-to-manage-risk-improve-security-posture-and-meet-compliance-requirements-1027570669.

[28] *Id.*

[29] *Id.*

including for providing or arranging services, treatment, running its organization, and billing for services.[30]

112. Additionally, CareCentrix vaguely acknowledges that it "will let you know promptly if a breach occurs that may have compromised the privacy or security of your Health Information."[31]

E. Defendant Failed to Exercise Due Care

113. Defendant failed to exercise due care in protecting patients' Personal Information by contracting with AMCA to handle debt collections for it.

114. AMCA's bankruptcy filings show how thinly capitalized the company was and how deficient its information technology ("IT") department and infrastructure were. Public reporting suggested that AMCA was not a reputable or responsible business associate—let alone an associate to be trusted with Plaintiffs' and Class Members' Personal Information.

115. Specifically, AMCA's bankruptcy filings admit that AMCA had less than $4 million in liquidity and its owner had to take a secured loan from his own personal money simply to mail notices to those impacted by the Data Breach. Put simply, Defendant should not have contracted and shared Plaintiffs' and Class Members' Personal Information with an entity that did not even have the means to mail notices to people affected by the Data Breach without having to file for bankruptcy.

116. The duration of time between the Data Breach and AMCA's claimed discovery of the Data Breach indicates that AMCA's systems to detect intrusion, detect unusual activity, and

[30] CareCentrix Notice of Privacy Practices, https://www.carecentrix.com/wp-content/uploads/Notice-of-Privacy-Practices-071219-Final.pdf (last accessed Nov. 4, 2019).

[31] *Id.*

log and report such events were woefully inadequate and not in compliance with industry standards. For example, according to technology-security company FireEye, the median amount of time between when a data breach occurs and when it is detected was 78 days in 2018. This number has consistently been on a downward trend in recent years due to improvements in detection computer technology.[32] The fact that it took AMCA at least 242 days to detect the Data Breach—nearly 3.5 times the median time for detection in 2018—is direct evidence of its failure to employ reasonable, industry-standard data security practices to safeguard Plaintiffs' and Class Members' Personal Information. AMCA's myriad data security deficiencies would have been readily apparent had CareCentrix conducted reasonable due diligence on AMCA's data security practices before contracting with and providing AMCA sensitive PHI and PII.

117. AMCA's inability to detect its own Data Breach, when an unrelated security firm (Gemini Advisory, which was not working for AMCA) was apparently able to do so with ease, is further evidence of the fact that AMCA employed inadequate data-security practices. It is also further evidence of CareCentrix's failure to conduct appropriate oversight of its business associates with whom it entrusted Plaintiffs' and Class Members' Personal Information.

118. Defendant's lack of oversight and failure to ensure that its HIPAA business associate employed reasonable and industry-standard data security measures, made the Data Breach foreseeable and preventable, had Defendant undertaken appropriate steps to oversee and ensure that AMCA could provide reasonable security for Plaintiffs' and Class members' Personal Information. The FireEye report indicates that in 2018, the median amount of time that it took a

[32] *M-Trends 2019: FireEye Mandiant Services Special Report, available at* https://content.fireeye.com/m-trends (last visited June 11, 2019).

third-party (like Gemini Advisory) to detect a data breach was three times the median time for internal detection.[33]

119. One of the easiest ways to minimize exposure to a data breach is to limit the type and amount of information provided to third-party business associates and routine destruction or archiving of inactive PII and PHI so that it cannot not be accessed through online channels. Access to millions of patient records through AMCA's online portal should not have been possible, had AMCA maintained appropriate protections. The sheer number of records suggests that AMCA was not destroying or archiving inactive records. Again, Defendant would have discovered AMCA's lax security practices had it exercised adequate oversight over its business associates and audited AMCA's data security processes and procedures.

120. Moreover, AMCA did not need access to Plaintiffs' PHI to collect payments. Instead, AMCA only needed the name of the vendor (CareCentrix), the invoice number, amount owed, and date of service to perform its collection services. But Defendant nevertheless regularly provided full account information that included PHI, apparently because it was more expedient than providing the narrower data set to AMCA.

121. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit payment card data. These standards are known as the Payment Card Industry Data Security Standard ("PCI DSS"). AMCA was not encrypting payment card information according to minimum industry standards of PCI DSS.

---

[33] *Id.*

122. The payment card industry has published a guide on point-to-point encryption and its benefits in securing payment card data: "point-to-point encryption (P2PE) solution cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption. By using P2PE, account data (cardholder data and sensitive authentication data) is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach."[34]

123. Defendant had an obligation to exercise oversight over AMCA in a manner that would include immediate knowledge of any data security incidents experienced by AMCA that could affect Defendant's patients. For example, AMCA pointed to the fact that it learned of the unauthorized access in March 2019 through a series of CPP notices suggesting that a "disproportionate number of credit cards that at some point had interacted with [AMCA's] web portal were later associated with fraudulent charges." However, Defendant did not learn of the unauthorized access until months later - in May 2019.

124. Defendant agreed, and had continuing contractual and common-law duties and obligations, to keep confidential the Personal Information its patients disclosed to it and to protect this information from unauthorized disclosure. Defendant's agreements, duties, and obligations are based on: (1) HIPAA; (2) industry standards; (3) the agreements and promises made to Plaintiffs and Class Members; and (4) Section 5(a) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Class Members provided their Personal Information to Defendant with the reasonable belief that Defendant and its business associates would comply with their agreements

[34] *Securing Account Data with the PCI Point –to-Point Encryption Standard v2*, available at https://www.pcisecuritystandards.org/documents/P2PE_At_a_Glance_v2.pdf (last accessed June 11, 2019).

and any legal requirements to keep that Personal Information confidential and secure from unauthorized disclosure.

125. HIPAA requires that Defendant provide every patient it treats, including Plaintiffs and Class Members, with a privacy notice.

126. As described herein, Defendant's privacy notices informed Plaintiffs and Class Members that the Defendant would safeguard and protect PII and PHI, and that Defendant could only use or share PHI for specific purposes.

127. As alleged above, AMCA was a "business associate" of Defendant with whom Defendant shared its patients' Personal Information. As Defendant's business associate, AMCA was required to maintain the privacy and security of Plaintiffs' and Class Members' Personal Information. HIPAA mandates that a covered entity (*i.e.*, Defendant) may only disclose PHI to a "business associate" (*i.e.*, AMCA) if the covered entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations.[35] Defendant failed to ensure that its business associate, AMCA, safeguarded Personal Information of Defendant's patients and that AMCA complied with HIPAA's privacy mandates.

128. CareCentrix's Business Associate Agreement ("BAA") with AMCA required AMCA to implement appropriate safeguards to prevent the misuse of Plaintiffs' Personal Information and permitted CareCentrix to audit AMCA's security practices to protect Plaintiff's Personal Information.

[35] *See* 45 C.F.R. §§ 164.502(e), 164.504(e), 164.532(d) and (e).

129. Beginning in 2015, CareCentrix also required AMCA to enter into a Vendor Security Requirements Agreement (VSRA), requiring certain security measures to be in place to secure Plaintiffs' Personal Information. CareCentrix, however, only adopted the VSRA because it was "being pushed onto CareCentrix by its clients."[36]

130. As part of the VSRA, CareCentrix submitted annual vendor security questionnaires to AMCA. While the questionnaires required AMCA to provide information about the security measures it had in place, according to AMCA, it "was pretty easy and straightforward" to complete without "too much trouble."[37]

131. The VSRA and vendor security questionnaires required AMCA to self-attest that it had the required security measures in place to secure Plaintiffs' Personal Information.

132. To ensure compliance with the VSRA, CareCentrix was permitted to conduct security audits, request report summaries of vulnerability scans and confirmation of remediation for vulnerabilities, require third-party risk assessments, require annual third-party penetration testing, and to request evidence of compliance.

133. While CareCentrix had these contractual rights to ensure that AMCA's security practices met industry-standards and were sufficient to protect Plaintiffs' Personal Information, CareCentrix did nothing to confirm that AMCA's self-attestations were even true.

134. CareCentrix failed to exercise its contractual rights to ensure that AMCA employed required security measures, despite being on notice of several data security deficiencies by AMCA. For example, AMCA sent CareCentrix unsecured emails with patient specific information in violation of HIPAA, AMCA informed CareCentrix that it did not maintain a SOC I Control Audit

[36] *See* AMCAPROD00704225

[37] *See* AMCAPROD00770937.

Report, as required by the BAA, and CareCentrix knew that AMCA did not maintain policies and procedures for compliance with consumer protection laws, including the Telephone Consumer Protection Act (TCPA).[38]

135. Had CareCentrix taken any appropriate and reasonable steps to confirm if AMCA's self-attestations with respect to the VSRA were in fact true, it would have easily discovered that AMCA's security practices, policies, and procedures were woefully inadequate and did not comply with the requirements that CareCentrix itself implemented, as part of the VSRA, at the behest of its clients.

F. Defendant Violated HIPAA's Requirements to Safeguard Data

136. Defendant had non-delegable duties to ensure that all information it collected and stored was secure, and that any associated entities with whom it shared member information maintained adequate and commercially-reasonable data security practices to ensure the protection of plan members' Personal Information.

137. Defendant is covered by HIPAA (*see* 45 C.F.R. § 160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

138. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the

[38] *See* AMCAPROD00194800; AMCAPROD00736482; AMCAPROD00134471.

information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. § 160.103.

139. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

140. HIPAA requires that Defendant implement appropriate safeguards for this information.

141. HIPAA further mandates that covered entities such as Defendant may disclose PHI to a "business associate," such as AMCA, *only* if the covered entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and assist in compliance with HIPAA privacy obligations.[39]

142. HIPAA requires that Defendant provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—*i.e.,* non-encrypted data.

143. Despite these requirements, Defendant failed to comply with its duties under HIPAA and its own Privacy Practices. Indeed, Defendant failed to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protect Plaintiffs' and the Class Members' Personal Information;

[39] *See* 45 C.F.R. §§ 164.502(e), 164.504(e), 164.532(d) and (e).

c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. Take safeguards to ensure that Defendant's business associates adequately protect protected health information;

i. Ensure compliance with the electronically protected health information security standard rules by its workforce, in violation of 45 C.F.R. § 164.306(a)(4); and/or

j. Train all members of its workforce effectively on the policies and procedures with respect to protected health information as necessary and

appropriate for the members of its workforce to carry out its functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

144. Defendant failed to comply with its duties under HIPAA and its own privacy policies despite being aware of the risks associated with unauthorized access of Plaintiffs' and Class Members' Personal Information.

G. Defendant Was on Notice That Highly Valuable Personal Information of its Patients Could Be Breached

145. Defendant was, or should have been, aware that it was collecting highly valuable data, for which Defendant knew, or should have known, there is an upward trend in data breaches in recent years.[40] Accordingly, Defendant was on notice of the harms that could ensue if it failed to protect Plaintiffs' and Class Members' Personal Information.

146. HHS' Office for Civil Rights currently lists 550 breaches affecting 500 or more individuals in the past 24 months.[41] CareCentrix has the eleventh-highest number of patients damaged by this Data Breach.[42]

147. As early as 2014, the FBI alerted the healthcare industry that they were an increasingly preferred target of hackers, stating "[t]he FBI has observed malicious actors targeting

---

40 *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Sept. 27, 2019) ("Our healthcare statistics clearly show there has been an upward trend in data breaches over the past 9 years, with 2018 seeing more data breaches reported than any other year since records first started being published.").

41 *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,* U.S. Dep't of Health and Human Services, Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Oct. 9, 2019).

42 *Id.*

healthcare related systems, perhaps for the purpose of obtaining Protected Health Information (PHI) and/or Personally Identifiable Information (PII)" so that these companies can take the necessary precautions to thwart such attacks.[43]

148. The co-founder of Lastline, a network security provider, said that "Hackers target financial companies, like this billing collection company, as they often store sensitive financial information that can be turned into immediate gains."[44]

149. At the end of 2018, the healthcare sector ranked second highest in the number of data breaches among measured sectors, and had the highest rate of exposure for each breach.[45] With this Data Breach, 2019 has seen the exposure of three times the number of records compromised in 2018.[46]

150. Other experts have stated that the Data Breach is at "the intersection of three of the types of data that hackers most desire: personal identifying information that can be used for identity fraud, information about medical conditions, and financial account information."[47]

---

43 Reuters, *FBI warns healthcare firms they are targeted by hackers*, August 20, 2014, http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820 (last visited Sept. 27, 2019).

44 Christopher Rowland, *Quest Diagnostics discloses breach of patient records*, WASH. POST, June 3, 2019, https://www.washingtonpost.com/business/economy/quest-diagnostics-discloses-breach-of-patient-records/2019/06/03/aa37b556-860a-11e9-a870-b9c411dc4312_story.html?utm_term=.78dd30c03a88 (last visited Sept. 27, 2019).

45 *2018 End-of-Year Data Breach Report*, Identity Theft Resource Center, https://www.idtheftcenter.org/2018-data-breaches (last visited Apr. 21, 2019).

46 *Healthcare Data Breach Statistics* (August 2019), HIPPAA Journal, https://www.hipaajournal.com/august-2019-healthcare-data-breach-report (last visited Sept. 27, 2019).

47 Scott Ikeda, *Third Party Data Breach Hits Quest Diagnostics with 12 Million Confidential Patient Records Exposed*, CPO Magazine, June 11, 2019, https://www.cpomagazine.com/cyber-security/third-party-data-breach-hits-quest-diagnostics-with-12-million-confidential-patient-records-exposed/ (last visited Oct. 7, 2019).

151. This same article has asked: "why did a collections agency have all of this information in the first place?" It also questioned why medical information and Social Security Numbers needed to be provided to debt collectors.[48]

152. Further, Cathy Allen, CEO of Shared Assessments, a cyber-risk management group, stated that "just the types of test proscribed might indicate a type of illness that you would not want employers or insurance companies to have. Thieves often steal and resell insurance data on the internet . . . having other information makes the data more valuable and the price higher."[49]

153. Personal Information is a valuable commodity to identity thieves. Compromised Personal Information is traded on the "cyber black-market." As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, social security numbers and other Personal Information directly on various dark web[50] sites making the information publicly available.[51]

---

48 *Id.*

49 *Id.*

50 The dark web refers to encrypted content online that cannot be found using conventional search engines and can only be accessed through specific browsers and software. MacKenzie Sigalos, *The dark web and how to access it* (Apr. 14, 2018), https://www.cnbc.com/2018/04/13/the-dark-web-and-how-to-access-it.html (last accessed June 17, 2019).

51 *Here's How Much Your Personal Information Is Selling for on the Dark Web,* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited June 17, 2019); McFarland et al., *The Hidden Data Economy*, at 3, *available at* https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf (last visited June 17, 2019).

154. Further, medical databases are particularly high value targets for identity thieves. According to one report, a stolen medical identity has a $50 street value on the black market, whereas a Social Security number sells for only $1.[52]

155. Healthcare data is especially valuable on the black market. According to one report, a healthcare data record may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[53]

156. According to a *Reuters* investigation that included interviews with nearly a dozen healthcare executives, cybersecurity investigators, and fraud experts, medical data for sale on underground markets "includes names, birth dates, policy numbers, diagnosis codes and billing information" which fraudsters commonly use "to create fake IDs to buy medical equipment or drugs that can be resold, or they combine a patient number with a false provider number and file made-up claims with insurers."[54]

157. According to Tom Kellermann, chief cybersecurity officer of cybersecurity firm Carbon Black, "Health information is a treasure trove for criminals [because] by compromising it, by stealing it, by having it sold, you have seven to 10 personal identifying characteristics of an

---

[52] *Study: Few Aware of Medical Identity Theft Risk*, Claims Journal (June 14, 2012), https://www.claimsjournal.com/news/national/2012/06/14/208510.htm (last visited June 10, 2019).

[53] *Hackers, Breaches, and the Value of Healthcare Data* (Feb. 02, 2022), https://www.securelink.com/blog/healthcare-data-new-prize-hackers/ (last visited Mar. 21, 2022).

[54] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924 (last visited Jan. 7, 2022).

individual."[55] For this reason, a patient's full medical records can sell for up to $1,000 on the dark web, while credit card numbers and Social Security numbers may cost $5 or less.[56]

158. As noted by Paul Nadrag, a software developer for medical device integration and data technology company Capsule Technologies: "The reason for this price discrepancy—like any other good or service—is perceived value. While a credit card number is easily canceled, medical records contain a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information. Once records are stolen, cybercriminals often tap into members of a criminal network on the dark web experienced in drug trafficking and money laundering who are eager to buy medical records to support their criminal activities, such as illegally obtaining prescription medications, filing bogus medical claims or simply stealing the patient's identity to open credit cards and fraudulent loans."[57]

159. Defendant is well aware that its own data and the data it shared with AMCA contains a treasure trove of material for threat actors as it has been targeted in the past. In March 2016, CareCentrix experienced a data breach when an unauthorized individual impersonated a

[55] *What Happens to Stolen Healthcare Data?* (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited Mar. 21, 2022).

[56] *Here's How Much Your Personal Information Is Selling for on the Dark Web* (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Mar. 21, 2022).

[57] *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web* (Jan. 26, 2021), https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web (last visited Mar. 21, 2022).

CareCentrix employee and obtained W-2 forms and other sensitive information.[58] Defendant was not a stranger to cyberattacks or theft of PII and PHI.

H. Defendant Has Harmed Plaintiffs and Class Members by Allowing Anyone to Access Their Personal Information

160. Defendant caused harm to Plaintiffs and Class Members by sharing their Personal Information with AMCA without properly monitoring its business associate, and AMCA failed to prevent attackers from accessing and stealing this information in the Data Breach.

161. Given the sensitive nature of the Personal Information stolen in the Data Breach—including names, mailing addresses, phone numbers, dates of birth, Social Security numbers, information related to Plaintiffs' and Class Members' medical providers and services (such as dates of service, and referring doctor) and other personal information (such as credit and debit card numbers, bank account information, insurance, insurance subscriber identification number), hackers have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future.

162. In fact, many victims of the Data Breach have already experienced harms as the result of the Data Breach, including, but not limited to, identity theft, financial fraud, tax fraud, unauthorized lines of credit opened in their names, medical and healthcare fraud, and unauthorized access to their bank accounts. Plaintiffs and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit protection services, contacting their financial institutions, checking credit reports, and spending time and effort searching for unauthorized activity.

---

[58] Amy Baxter, *Former CareCentrix Employee Continues Fight in Data Breach*, Home Health Care News (Apr. 16, 2017), https://homehealthcarenews.com/2017/04/former-carecentrix-employee-continues-fight-in-data-breach/.

163. The Personal Information exposed in the Data Breach is highly coveted and valuable on underground or black markets. For example, a cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground internet websites known as the "dark web"—and information tied to this Data Breach has already been offered for sale. Identity thieves can use the Personal Information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit medical and healthcare-related fraud; (h) access financial accounts and records; or (i) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest. Further, loss of private and personal health information can expose the victim to loss of reputation, loss of employment, blackmail, extortion, and other negative effects.

164. Medical data is particularly valuable to hackers. In June 2016, a hacker reportedly was offering to sell hacked medical records of nearly 700,000 patients for hundreds of thousands of dollars on a "deep web marketplace." [59] Later, the same hacker revealed that he had a database of 9.3 million records from a U.S. insurer that was for sale. [60]

165. While federal law generally limits an individual's liability for fraudulent credit card charges to $50, there are no such protections for a stolen medical identity. According to a 2015

---

[59] Healthcare under Attack: What Happens to Stolen Medical Records?, June 30, 2016, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/healthcare-under-attack-stolen-medical-records (last visited Sept. 27, 2019).

[60] Lording it over the healthcare sector: health insurer database with 9.3M entries up for sale, https://www.databreaches.net/lording-it-over-the-healthcare-sector-health-insurer-database-with-9-3m-entries-up-for-sale/, (last visited Sept. 27, 2019).

survey on medical identity theft conducted by the Ponemon Institute, victims of medical identity theft spent an average of $13,500 in out-of-pocket costs to resolve the crime.[61] Frequently, this information was used to obtain medical services or treatments (59%), obtain prescription drugs (56%), or receive Medicare and Medicaid benefits (52%). Only 14% of respondents said that the identity thieves used the information to obtain fraudulent credit accounts, indicating that medical information is a much more profitable market.[62]

166. According to the Ponemon study, "[t]hose who have resolved the crime spent, on average, more than 200 hours on such activities as working with their insurer or healthcare provider to make sure their personal medical credentials are secured and can no longer be used by an imposter and verifying their personal health information, medical invoices and claims and electronic health records are accurate."[63]

167. Additionally, the study found that medical identity theft can have a negative impact on reputation as 45% of respondents said that medical identity theft affected their reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions, with 19% responding that they missed out on employment opportunities as a result.[64]

168. Exacerbating the problem, victims of medical identity theft oftentimes struggle to resolve the issue because HIPAA regulations require the victim to be personally involved in the

[61] Ponemon Institute, *Fifth Annual Study on Medical Identity Theft*, https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65 (last visited Mar. 21, 2022).

[62] *Id*. at 9.

[63] *Id*. at 2.

[64] *Id*. at 14.

resolution of the crime.[65] In some cases, victims may not even be able to access medical records using their personal information because they include a false name or data points taken from another person's records. Consequently, only 10% of medical identity theft victims responded that they "achiev[ed] a completely satisfactory conclusion of the incident."[66]

169. Moreover, it can take months or years for victims to even discover they are the victim of medical-related identity theft or fraud given the difficulties associated with accessing medical records and healthcare statements. For example, the FTC notes that victims may only discover their identity has been compromised after they:

- Receive a bill for medical services they did not receive;
- Get contacted by a debt collector about medical debt they do not owe;
- See medical collection notices on their credit report that they do not recognize;
- Find erroneous listings of office visits or treatments on their explanation of benefits (EOB);
- Receive information from their health plan that they have reached their limit on benefits; or
- Be denied insurance because their medical records show a condition they do not have.[67]

170. Other types of medical fraud include "leveraging details specific to a disease or terminal illness, and long-term identity theft."[68] According to Tom Kellermann, "Traditional

---

[65] *Id*. at 1.

[66] *Id*.

[67] FTC, *Medical Identity Theft FAQs for Health Care Providers and Health Plans*, https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf (last visited Mar. 21, 2022).

[68] *What Happens to Stolen Healthcare Data?* (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited Mar. 21, 2022).

criminals understand the power of coercion and extortion. By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[69] Long-term identity theft occurs when fraudsters combine a victim's data points, including publicly-available information or data points exposed in other data breaches, to create new identities, open false lines of credit, or commit tax fraud that can take years to remedy.

171. In a data breach implicating a medical provider or medical information, consumers face the additional risk of their Health Savings Accounts ("HSAs") being compromised. HSAs are often tied to specialized debit cards used to make medical-based payments. However, they can also be used for regular purchases (albeit incurring a severe tax penalty). Such information is an "easy target" for criminal actors.[70]

172. Fraudulent charges have already been linked to Defendant's billing collector's data handling. Another lab impacted by the Data Breach publicly revealed the exposure of patients' Personal Information only after "a disproportionate number of credit cards that at some point had interacted with [AMCA's] web portal were later associated with fraudulent charges."[71]

173. In addition, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or

---

[69] *Id*.

[70] *Id.*

[71] Declaration of Russell H. Fuchs Pursuant to Local Bankruptcy Rule 1007-2 and in Support of "First Day" Motions, *In re Retrieval-Masters Creditors Bureau, Inc.*, No. 19-23185-RDD (Bankr. S.D.N.Y. June 17, 2019), ECF No. 2 at 5-6.

mortgages.[72] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

174. As explained further by the FTC, medical identity theft can have other serious consequences:

> Medical ID thieves may use your identity to get treatment—even surgery—or to bilk insurers by making fake claims. Repairing damage to your good name and credit record can be difficult enough, but medical ID theft can have other serious consequences. If a scammer gets treatment in your name, that person's health problems could become a part of your medical record. It could affect your ability to get medical care and insurance benefits, and could even affect decisions made by doctors treating you later on. The scammer's unpaid medical debts also could end up on your credit report.[73]

175. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[74]

176. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. losing the inherent value of their Personal Information;

---

[72] *The Aftermath 2017*, Identity Theft Resource Center, https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited Aug. 9, 2019).

[73] *Medical ID Theft: Health Information for Older People*, Federal Trade Commission, *available at* https://www.consumer.ftc.gov/articles/0326-medical-id-theft-health-information-older-people (last visited Oct. 7, 2019).

[74] *See Study: Medical identity theft is costly for victims,* CNET (Mar. 3, 2010), *available at* https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Oct. 11, 2019).

b. identity theft and fraud resulting from the theft of their Personal Information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

h. the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

177. Even in instances where a consumer is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement that is not refunded. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[75]

178. There may also be a significant time lag between when Personal Information is stolen and when it is actually misused. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[76]

179. Plaintiffs and Class Members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that

---

[75] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Aug. 9, 2019).

[76] U.S. Gov't Accountability Off., GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown* (2007), *available at* http://www.gao.gov/new.items/d07737.pdf.

has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[77]

180. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, Defendant would have no reason to tout its data security efforts to their actual and potential customers.

181. Consequently, had consumers known the truth about Defendant's data security practices—that it did not adequately protect and store their Personal Information—they would not have entrusted their Personal Information to CareCentrix.

182. Reactions to the Data Breach reflect the severity and breadth of the adverse impact on the American public.

183. The Attorney General of Maryland issued a "Consumer Alert" on June 12, 2019, warning residents that 500,000 CareCentrix patients were affected by the Data Breach. "Massive data breaches like the one experienced by the AMCA are extremely alarming, especially considering the likelihood that personal, financial, and medical information may now be in the hands of thieves and scammers," said Attorney General Frosh. "I strongly urge consumers to take steps to ensure that their information and personal identity is protected."[78]

184. Connecticut Attorney General William Tong, announcing that Illinois and Connecticut's Attorneys General have opened an investigation into the Data Breach, stated:

---

[77] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited Aug. 9, 2019).

[78] Brian E. Frosh, Attorney General, Maryland, Consumer Alert (June 12, 2019), http://www.marylandattorneygeneral.gov/press/2019/061219.pdf.

> The last thing patients should have to worry about is whether their personal information has been compromised by the entities responsible for protecting it. I am committed to ensuring that impacted patients receive timely notification and that the companies involved take precautions to protect consumers' sensitive health and financial information in the future.[79]

185. Other State Attorneys General, including the Attorneys General of Michigan, Minnesota, and North Carolina, have also launched investigations into the Data Breach.[80]

CLASS ACTION ALLEGATIONS
NATIONWIDE CLASSES

186. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

> All natural persons residing in the United States whose Personal Information was compromised in the Data Breach**.**

187. The Nationwide Class asserts claims against Defendant for negligence (Count 1), negligence *per se* (Count 2), breach of confidence (Count 3), invasion of privacy – intrusion upon seclusion (Count 4), and unjust enrichment (Count 5). The Class also asserts claims against Defendant CareCentrix for violations of the Connecticut Unfair Trade Practices Act, C.G.S.A. §§ 42-110G, *et seq.* (Count 6), and for Breach of Security Regarding Computerized Data, C.G.S.A. §§ 36a-701b, *et seq.* (Count 7).

---

79 *Connecticut and Illinois Open Investigation into Quest Diagnostics, LabCorp Data Breach*, The Office of Attorney General William Tong, *available at* https://portal.ct.gov/AG/Press-Releases/2019-Press-Releases/CT-AND-IL-OPEN-INVESTIGATION-INTO-QUEST-AND-LABCORP-DATA-BREACH.

80 *AMCA Data Breach Tally Passes 20 Million as BioReference Laboratories Added to List of Impacted Entities*, HIPPA Journal, https://www.hipaajournal.com/amca-data-breach-tally-passes-20-million-as-bioreference-laboratories-added-to-list-of-impacted-entities/ (last visited Oct. 9, 2019).

STATEWIDE SUBCLASSES

188. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of state-by-state claims in the alternative to the nationwide claims, as well as statutory claims under state data breach statutes and consumer protection statutes (Counts 8 and 9), on behalf of separate statewide subclasses for each (the "Statewide Subclasses"), defined as follows:

> All natural persons residing in that specific state whose Personal Information was compromised in the Data Breach.

189. Excluded from the Nationwide Class and each Statewide Subclass are the Defendant, any entity in which the Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and each Statewide Subclass are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

190. **Numerosity: Federal Rule of Civil Procedure 23(a)(1)**. The members of each Class and Subclass are so numerous and geographically dispersed that individual joinder of all Class Members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, approximately 500,000 CareCentrix patients had their data compromised in the Data Breach. Those individuals' names and addresses are available from Defendant's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. On information and belief, there are at least thousands of Class Members in each Statewide Subclass, making joinder of all Statewide Subclass members impracticable.

191. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The common questions include:

a. Whether Defendant had a duty to protect Personal Information;

b. Whether Defendant failed to take reasonable and prudent security measures;

c. Whether Defendant knew or should have known of the susceptibility of AMCA's systems to a data breach;

d. Whether Defendant was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Defendant's security measures to protect its systems were reasonable in light of known legal requirements;

f. Whether Defendant was negligent in failing to adequately monitor and audit the data security systems of its vendors and business associates;

g. Whether Defendant's efforts (or lack thereof) to ensure the security of patients' Personal Information provided to business associates were reasonable in light of known legal requirements;

h. Whether Defendant's conduct constituted unfair or deceptive trade practices;

i. Whether Defendant violated state law when it failed to implement reasonable security procedures and practices;

j. Which security procedures and notification procedures Defendant should be required to implement;

k. Whether Defendant has a contractual obligation to use reasonable security measures;

l. Whether Defendant has complied with any contractual obligation to use reasonable security measures;

m. What security measures, if any, must be implemented by Defendant to comply with its contractual obligations;

n. Whether Defendant violated state consumer protection and state medical information privacy laws in connection with the actions described herein;

o. Whether Defendant failed to notify Plaintiffs and Class Members as soon as practicable and without delay after the Data Breach was discovered;

p. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach of AMCA's systems and/or the loss of the Personal Information of Plaintiffs and Class Members;

q. Whether Plaintiffs and Class Members were injured and suffered damages or other losses because of Defendant's failure to reasonably protect their Personal Information; and,

r. Whether Plaintiffs and Class Members are entitled to damages, declaratory relief, or injunctive relief.

192. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiffs' claims are typical of those of other Class Members. Plaintiffs' Personal Information was in Defendant's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to other Class Members and Plaintiffs seek relief consistent with the relief of the Class.

193. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class because Plaintiffs are members of the Class and are committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

194. **Predominance & Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

195. **Risk of Prosecuting Separate Actions.** This case is appropriate for certification because prosecuting separate actions by individual proposed Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for Defendant or would be dispositive of the interests of members of the proposed Class.

196. **Ascertainability.** The Class and Subclasses are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the class. The Class and Subclasses consist of individuals who received services from Defendant and whose accounts were placed into collections with AMCA by Defendant. Class Membership can be determined using Defendant's and AMCA's records in their databases.

197. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiffs seek prospective injunctive relief as a wholly separate remedy from any monetary relief.

198. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

b. Whether Defendant failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiffs and the Class Members;

c. Whether Defendant failed to adequately monitor and audit the data security systems of their vendors and business associates;

d. Whether adherence to HIPAA regulations, FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1

NEGLIGENCE

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

199. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

200. Defendant required Plaintiffs and Class Members to submit Personal Information to obtain diagnostic and medical services, which Defendant provided to AMCA for billing purposes. Defendant collected and stored the Personal Information for commercial gain.

201. Defendant knew or should have known that AMCA's systems were vulnerable to unauthorized access and exfiltration by third parties.

202. Defendant had non-delegable duties to ensure that contractual partners with whom they shared patient information maintained adequate and commercially-reasonable data security practices to ensure the protection of patients' Personal Information.

203. Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' Personal Information within its control from being compromised, lost, stolen, accessed and misused by unauthorized persons.

204. Defendant owed a duty of care to Plaintiffs and members of the Class to provide security, consistent with industry standards, to ensure that the systems and networks adequately protected the Personal Information.

205. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and the Plaintiffs and Class Members. The special relationship arose because Plaintiffs and Class Members entrusted Defendant with their confidential data as part of the health treatment process. Only Defendant was in a position to ensure that its contractual partners had sufficient safeguards to protect against the harm to Plaintiffs and Class Members that would result from a data breach.

206. Defendant's duty to use reasonable care in protecting Personal Information arose as a result of the common law and the statutes and regulations, as well as their own promises regarding privacy and data security to its patients. This duty exists because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. By collecting and maintaining personal and confidential information of Plaintiffs and Class Members, and acknowledging that this information needed to be kept secure, it was foreseeable that they would be harmed in the future if Defendant did not protect Plaintiffs' and Class Members' Personal Information from hackers.

207. Defendant's duties also arose under HIPPA regulations, which, as described above, applied to Defendant and establish national standards for the protection of patient information, including protected health information, which required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The duty also arose under HIPAA's Privacy Rule

requirement that Defendant obtain satisfactory assurances from its business associate AMCA that AMCA would appropriately safeguard the protected health information it receives or creates on behalf of the Defendant. 45 C.F.R. §§ 164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

208. Defendant's duties also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal and confidential information. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, several individual states have enacted statutes based upon the FTC Act that also created a duty.

209. Defendant knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities of its vendors' and business associates' systems, and the importance of adequate security.

210. Defendant breached its common law, statutory, and other duties—and thus were negligent—by failing to use reasonable measures to protect patients' Personal Information, and by failing to provide timely and adequately detailed notice of the Data Breach.

211. Defendant breached its duties to Plaintiffs and Class Members in numerous ways, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiffs' and Class Members' Personal Information;

b. Failing to comply with industry standard data security standards during the period of the Data Breach;

c. Failing to adequately monitor and audit the data security systems of its vendors and business associates;

d. Failing to comply with regulations protecting the Personal Information at issue during the period of the Data Breach;

e. Failing to adequately monitor, evaluate, and ensure the security of AMCA's network and systems;

f. Failing to recognize in a timely manner that Plaintiffs' and other Class Members' Personal Information had been compromised; and

g. Failing to timely and adequately disclose that Plaintiffs' and Class Members' Personal Information had been improperly acquired or accessed.

212. Plaintiffs' and Class Members' Personal Information would not have been compromised but for Defendant's wrongful and negligent breach of their duties.

213. Defendant's failure to take proper security measures to protect sensitive Personal Information of Plaintiffs and Class Members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Personal Information of Plaintiffs and Class Members.

214. It was also foreseeable that Defendant's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiffs and other Class Members.

215. Neither Plaintiffs nor the other Class Members contributed to the Data Breach and subsequent misuse of their Personal Information as described in this Complaint.

216. As a direct and proximate cause of Defendant's conduct, Plaintiffs and the Class suffered damages and will suffer damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained

through the use of the Personal Information of Plaintiffs and Class Members; damages arising from identity theft or fraud; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take years to discover and detect; and loss of the value of their privacy and confidentiality of the stolen confidential data, including health data.

COUNT 2

NEGLIGENCE PER SE

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

217. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

218. Defendant is an entity covered by HIPAA (45 C.F.R. § 160.102) and as such are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

219. HIPAA requires Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). HIPAA also requires Defendant to obtain satisfactory assurances that their business associates would appropriately safeguard the protected health information it receives or

creates on behalf of the Defendant. 45 C.F.R. §§ 164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA. AMCA constitutes a "business associate" within the meaning of HIPAA.

220. HIPAA further requires Defendant to disclose the unauthorized access and theft of the Personal Information to Plaintiffs and the Class Members "without unreasonable delay" so that Plaintiffs and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Personal Information. *See* 45 C.F.R. §§ 164.404, 406, 410.

221. Defendant violated HIPAA by failing to reasonably protect Plaintiffs' and Class Members' Personal Information, as described herein.

222. Defendant's violations of HIPAA constitute negligence per se.

223. Plaintiffs and Class Members are within the class of persons that HIPAA was intended to protect.

224. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

225. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Personal Information. 15 U.S.C. § 45(a)(1).

226. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

227. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards.

Defendant's conduct was particularly unreasonable given the nature and amount of Personal Information they obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving companies as large as Defendant, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

228. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

229. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

230. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

231. As a direct and proximate result of Defendant's negligence per se under HIPAA and the FTC Act, Plaintiffs and the Class have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein.

COUNT 3

BREACH OF CONFIDENCE

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

232. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

233. Plaintiffs and Class Members maintained a confidential relationship with Defendant because Plaintiffs and Class Members provided Defendant with their Personal Information that was confidential and novel, highly personal and sensitive, and not generally

known. The confidential relationship required Defendant to undertake a duty to not to disclose the Personal Information to unauthorized third parties.

234. Defendant knew Plaintiffs' and Class Members' Personal Information was disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the Personal Information it collected, stored, and maintained.

235. The Data Breach was an unauthorized disclosure of Plaintiffs' and the Class Members' Personal Information in violation of this understanding. The unauthorized disclosure occurred because Defendant failed to implement and maintain reasonable safeguards to protect the Personal Information in their possession and failed to comply with industry-standard data security practices.

236. The unconsented disclosure of the Personal Information to an unauthorized third party harmed Plaintiffs and Class Members.

237. As a direct and proximate result of Defendant's breach of confidence, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT 4

INVASION OF PRIVACY – INTRUSION UPON SECLUSION

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

238. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

239. Defendant intentionally intruded into Plaintiffs' and Class Members' seclusion by disclosing, without permission, their Personal Information to a third party that was unequipped and unable to keep their Personal Information secure.

240. By failing to keep Plaintiffs' and Class Members' Personal Information secure, and disclosing the Personal Information to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiffs' and Class Members' privacy right to seclusion by, *inter alia*:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. Invading their privacy by improperly using their Personal Information properly obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

c. Failing to adequately secure their Personal Information from disclosure to unauthorized persons; and

d. Enabling the disclosure of their Personal Information without consent.

241. The Personal Information publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial, health, and treatment information.

242. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein.

243. Plaintiffs and Class Members alternatively seek an award of nominal damages.

COUNT 5

UNJUST ENRICHMENT
On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

244. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

245. For years and continuing to today, Defendant's business model has depended upon patients entrusting them with their Personal Information. Trust and confidence are critical and central to both the services provided by CareCentrix to patients and the billing and collection for such services. Unbeknownst to Plaintiffs and Class Members, however, Defendant failed to ensure its vendors and business associates reasonably or adequately secured, safeguarded, and otherwise protected Plaintiffs' and Class Members' Personal Information. Defendant's deficiencies described herein were contrary to its security messaging.

246. Plaintiffs and Class Members engaged CareCentrix for services and provided Defendant with, and allowed Defendant to collect, their Personal Information on the mistaken belief that Defendant complied with its duty to safeguard and protect patients' Personal Information. Putting its short-term profit ahead of safeguarding Personal Information, and unbeknownst to Plaintiffs and Class Members, Defendant knowingly sacrificed security in favor of collecting moneys Defendant believed it was owed. Defendant knew that the manner in which it maintained and transmitted patients' Personal Information violated its fundamental duties to Plaintiffs and Class Members by disregarding industry-standard security protocols to ensure confidential information was securely transmitted and stored.

247. Defendant had within its exclusive knowledge at all times relevant that its vendors and business associates failed to implement adequate security measures to keep patients' Personal

Information secure. This information was not available to Plaintiffs, Class Members, or the public at large.

248. Defendant also knew that Plaintiffs and Class Members expected that their information would be kept secure against known security risks and that the security protocols of any vendors or business associates used by Defendant would be thoroughly vetted before they were given patients' Personal Information.

249. Plaintiffs and Class Members did not expect that Defendant would engage a billing collection agency, AMCA, that employed substantially deficient security protocols and would store highly sensitive PHI that was irrelevant to collecting payments.

250. Had Plaintiffs and Class Members known about Defendant's practice of sharing their Personal Information with vendors and business associates who were unequipped to protect it—and insecurely transmitting sensitive PHI that had no bearing on collecting payments—Plaintiffs and Class Members would not have engaged Defendant to perform any services and would never have provided Defendant with their Personal Information.

251. By withholding these material facts, Defendant put its own interests ahead of its patients' interests and benefitted itself to the detriment of Plaintiffs and Class Members.

252. As a result of Defendant's conduct as alleged herein, Defendant sold more services than it otherwise would have and was able to charge Plaintiffs and Class Members when it otherwise could not have. Defendant was unjustly enriched by charging and collecting for those services to the detriment of Plaintiffs and Class Members.

253. It would be inequitable, unfair, and unjust for Defendant to retain these wrongfully obtained benefits. Defendant's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

254. Defendant's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their private Personal Information.

255. Each Plaintiff and member of the proposed Classes is entitled to restitution and non-restitutionary disgorgement in the amount by which Defendant was unjustly enriched, to be determined at trial.

COUNT 6

CONNECTICUT UNFAIR TRADE PRACTICES ACT, C.G.S.A. § 42-110G, *et. seq.*
On Behalf of Plaintiffs and the Nationwide Class

256. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

257. Defendant and Plaintiffs are "persons" as defined by C.G.S.A. § 42-110a(3).

258. Defendant is engaged in "trade" or "commerce" as those terms are defined by C.G.S.A. § 42-110a(4).

259. At the time of filing this Complaint, Plaintiffs have sent notice to the Attorney General and Commissioner of Consumer Protection pursuant to C.G.S.A. § 42-110g(c). Plaintiffs will provide a file-stamped copy of the Complaint to the Attorney General and Commissioner of Consumer Protection.

260. Defendant advertised, offered, or sold services in Connecticut, and engaged in trade or commerce directly or indirectly affecting the people of Connecticut.

261. Defendant engaged in deceptive acts and practices and unfair acts and practices in the conduct of trade or commerce, in violation of the C.G.S.A. § 42-110b, including:

a. Representing that services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;

b. Representing that services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; and

c. Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce.

262. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

263. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

264. Had Defendant disclosed to Plaintiffs and Class Members that it misrepresented AMCA's vendor's network security, or otherwise had not omitted to Plaintiffs and Class Members that AMCA's systems were insecure, Defendant would not have been able to continue storing Plaintiffs and Class Members' Personal Information on its network, and would have been forced to disclose the material information regarding AMCA's security. Instead, Defendant failed to discover that AMCA's servers were vulnerable through adequate due diligence and testing, and yet still continued to provide AMCA with Plaintiffs' and Class Members' Personal Information.

265. Defendant's unlawful, deceptive, and unconscionable acts include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures

following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' Personal Information, including by implementing and maintaining reasonable security measures and ensuring its vendors and business associates maintained reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' Personal Information or ensure its vendors and business associates reasonably or adequately secured such information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information.

266. Defendant's conduct was intentional, knowing, and malicious because Defendant knew the value of Personal Information they stored and provided to AMCA and failed to undertake or implement necessary safeguards, controls, and data security measures to keep it secure.

267. Plaintiffs conferred a benefit on Defendant—payment for medical services—in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in

writing, or via electronic disclosure that did not reasonably ensure its billing collector AMCA adequately secured patients' Personal Information, Plaintiffs would not have sought or purchased services from Defendant.

268. As a direct and proximate result of Defendant's deceptive acts and practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; loss of value of Personal Information; time and money spent on preventative and corrective measures; and an increased, imminent risk of fraud and identity theft.

269. Defendant's deceptive acts and practices caused substantial, ascertainable injury to Plaintiffs and Class members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

270. The application of Connecticut law to the Class is appropriate, given CareCentrix's headquarters are in Connecticut; however, discovery will be necessary to address appropriately any choice of law issues.

271. Defendant's violations of Connecticut law were done with reckless indifference to Plaintiffs and the Class or were with an intentional or wanton violation of those rights.

272. Plaintiffs request damages in the amount to be determined at trial, including statutory and common law damages, restitution, attorneys' fees, and punitive damages.

COUNT 7

BREACH OF SECURITY REGARDING COMPUTERIZED DATA, C.G.S.A. § 36a-701b, *et. seq.*

On Behalf of Plaintiffs and the Nationwide Class

273. Plaintiffs repeat the allegations contained in the preceding paragraphs as if fully set forth herein.

274. Defendant is a business that conducts business in Connecticut and owns, licenses, and maintains computerized data that includes Personal Information as covered by C.G.S.A. § 36a-701b(b). Defendant also maintains computerized data that includes Personal Information that it does not own as covered by C.G.S.A. § 36a-701b(c).

275. Plaintiffs and Class Members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered by C.G.S.A. § 36a-701b(a).

276. Defendant is required to accurately notify Plaintiffs and Class members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay, not to exceed ninety days after discovery of the breach under C.G.S.A. § 36a-701b(b).

277. Defendant is required to immediately notify Plaintiffs and Class members if it becomes aware of a breach of its data security system which may have compromised personal information it stores but Plaintiffs and Class Members own under C.G.S.A. § 36a-701b(c).

278. Because Defendant was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by C.G.S.A. §§ 36a-701b(b) and (c).

279. By failing to disclose the Data Breach in an accurate and timely manner, Defendant failed to comply with C.G.S.A. §§ 36a-701b(b) and (c). Pursuant to C.G.S.A. § 36a-701b(g),

Defendant's failure to comply was an unfair trade practice under the Connecticut Unfair Trade Practices Act, C.G.S.A. §§ 42-110a, *et seq*.

280. As a direct and proximate result of Defendant's violations of C.G.S.A. §§ 36a-701b(b) and (c), Plaintiffs and Class members suffered damages, as described above.

281. Defendant's corporate office headquarters and the fact that it centers its operations in Connecticut makes it appropriate to assert this claim on behalf of the Class.

282. Plaintiffs and class members seek relief under C.G.S.A. § 42-110g for the harm they suffered because of Defendant's violations of C.G.S.A. §§ 36a-701b(b) and (c), including actual damages and equitable relief.

CLAIMS ON BEHALF OF STATE-SPECIFIC SUBCLASSES

283. In the alternative, the claims asserted above are also brought on behalf of statewide subclasses on behalf of those subclasses and for subclasses with substantially-similar state consumer protection laws.

COUNT 8

VIOLATIONS OF NEW YORK CONSUMER LAW FOR DECEPTIVE ACTS AND PRACTICES AND FALSE ADVERTISING, N.Y. GBL § 349, *et seq.*

On Behalf of Plaintiff Graifman and the New York Subclass

284. Plaintiff Graifman repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

285. Defendant engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including omitting, suppressing, and concealing the material fact that it did not reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and New York Subclass members' Personal Information.

286. Plaintiff and New York Subclass members were deceived in New York. They also transacted with Defendant in New York by utilizing Defendant's services in New York.

287. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of AMCA's data security and ability to protect the confidentiality of consumers' Personal Information.

288. Plaintiff and New York Subclass members conferred a benefit on Defendant—payment for medical services—in reliance on Defendant's omissions. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not reasonably ensure its billing collector AMCA adequately secured patients' Personal Information, Plaintiff and New York Subclass members would not have sought or purchased services from Defendant.

289. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiff and New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

290. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the hundreds of thousands, if not millions, of New Yorkers affected by the Data Breach.

291. The above deceptive and unlawful practices and acts by Defendant caused

substantial injury to Plaintiff and New York Subclass members that they could not reasonably avoid.

292. Plaintiff and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, restitution, injunctive relief, and attorney's fees and costs.

COUNT 9

VIOLATION OF NEW YORK'S DATA BREACH LAWS DELAYED NOTIFICATION, N.Y. GBL § 899-aa, *et seq.*

On Behalf of Plaintiff Graifman and the New York Subclass

293. Plaintiff Graifman repeats the allegations contained in the preceding paragraphs as if fully set forth herein.

294. Section 899-aa(3) of the New York General Business Law requires any "person or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization."

295. The security breach notification shall be directly provided to the affected persons by: (a) written notice; (b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction; (c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or (d) substitute notice, if a business

demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. N.Y. Gen. Bus. Law § 899-a (5).

296. The Security Breach described herein this Complaint constitutes a "breach of the security system" of Defendant and its agent AMCA.

297. As alleged above, Defendant unreasonably delayed informing Plaintiff and the New York Subclass about the Security Breach, affecting the confidential and non-public Private Information of Plaintiff and the New York Subclass after Defendant knew the Security Breach had occurred. AMCA learned of the breach on March 20, 2019, and CareCentrix did not notify Plaintiff until July 10, 2019.

298. Defendant failed to disclose to Plaintiff and the New York Subclass, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Private Information when Defendant knew or reasonably believed such information had been compromised.

299. Defendant's ongoing business interests gave it incentive to conceal the Security Breach from the public to ensure continued revenue.

300. Upon information and belief, no law enforcement agency instructed Defendant that notification to Plaintiff and the New York Subclass would impede Defendant's investigation.

301. As a result of Defendant's violation of New York law, Plaintiff and the New York Subclass were deprived of prompt notice of the Security Breach and were thus prevented from taking appropriate protective measures securing identity theft protection, or requesting a credit freeze. These measures would have prevented some or all of the damages the Plaintiff and the New

York Subclass suffered because their stolen information would not have any value to identity thieves.

302. As a result of Defendant's violation of New York law, Plaintiff and the New York Subclass have suffered incrementally increasing damages separate and distinct from those simply caused by the breaches themselves.

303. Plaintiff and the New York Subclass seek all remedies available under New York law, including, but not limited to, damages the Plaintiff and the New York Subclass suffered as alleged above, as well as equitable relief.

REQUESTS FOR RELIEF

Plaintiffs, individually and on behalf of members of the Class and Subclasses, as applicable, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Co-Lead and Co-Liaison Counsel as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

3. That the Court award Plaintiffs and Class and Subclass members compensatory, consequential, and general damages in an amount to be determined at trial;

4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of its unlawful acts, omissions, and practices;

5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

6. That Plaintiffs be granted the declaratory relief sought herein;

7. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

8. That the Court award pre- and post-judgment interest at the maximum legal rate; and

9. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

CARELLA, BYRNE, CECCHI,
OLSTEIN, BRODY & AGNELLO, P.C.
Interim Lead Counsel for Plaintiffs

By: /s/ James E. Cecchi
JAMES E. CECCHI

Dated: March 31, 2022

Joseph J. DePalma
Bruce D. Greenberg
LITE DEPALMA GREENBERG & AFANADOR LLC
570 Broad Street, Suite 1201
Newark, New Jersey 07102
(973) 623-3000

Amy E. Keller
Adam J. Levitt
DICELLO LEVITT GUTZLER LLC
10 North Dearborn Street, 11th Floor
Chicago, Illinois 60602
(312) 214-7900

Other Labs Track Co-Lead Counsel

James Pizzirusso
Katie R. Beran
HAUSFELD LLP
1700 K Street, NW, Suite 650
Washington, DC 20006
(202) 540-7200

Laurence D. King
Mario M. Choi
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, Suite 400
San Francisco, CA 94104
(415) 772-4700

Joseph P. Guglielmo

SCOTT+SCOTT ATTORNEYS AT LAW, LLP
The Helmsley Building
230 Park Ave, 17th Floor
New York, New York 10169
(212) 223-6444

Other Labs Track Steering Committee

Melissa R. Emert
KANTROWITZ, GOLDHAMER, & GRAIFMAN, P.C.
747 Chestnut Ridge Road, SUITE 200
Chestnut Ridge, NY 10977
(212) 687-7230

Jay I. Brody
KANTROWITZ, GOLDHAMER, & GRAIFMAN, P.C.
210 Summit Avenue
Montvale, New Jersey 07645
(201) 391-7000

Attorneys for Plaintiff Graifman